Notice of Allowability	Application No.	Applicant(s)	
	09/809,030	BEN-ITZHAK, YUVAL	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 6/8/07*.

2. ☒ The allowed claim(s) is/are *5-10,13,14,17-19,23,24,30,34,35,38-40,44 and 45*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/19/07* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. Claims 5-10, 13, 14, 17-19, 23, 24, 30, 34, 35, 38-40, 44 and 45 are allowed. Claims 5-10, 13, 14, 17-19, 23, 24, 30, 34, 35, 38-40, 44 and 45 are re-numbered as claims 1-22.

31,

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Todd Schneider on 7/19/07.

The application has been amended as follows:

3. 5. (Currently Amended) A method for protecting an application from executing an illegal or harmful operation request received from a distributed environment, the method comprising the steps of:

determining whether an operation request is illegal or harmful to an environment of an application, ~~and~~

preventing said application from executing an illegal or harmful operation request, wherein said step of preventing comprises the step of modifying said illegal or harmful operation request into a legal or harmless operation request~~.~~

comparing said operation request against stored known vulnerability patterns to determine a match, and

blocking said operation request if said match is found,

wherein said step of comparing comprises the steps of:

converting every consecutive specified number of characters in said operation request into n-bits of binary code;

computing a hash value for said every consecutive specified number of characters in said operation request; and

comparing every hash value to stored hash values representing vulnerability patterns.

4. 6. (Currently Amended) A method for protecting an application from executing an illegal or harmful operation request received from a distributed environment, the method comprising the steps of:

determining whether an operation request is illegal or harmful to an environment of an application, ~~and~~

preventing said application from executing an illegal or harmful operation request, wherein said step of preventing comprises the step of replacing said illegal or harmful operation request into a legal or harmless operation request~~.~~,

comparing said operation request against stored known vulnerability patterns to determine a match, and

blocking said operation request if said match is found,

wherein said step of comparing comprises the steps of:

converting every consecutive specified number of characters in said operation request into n-bits of binary code;

computing a hash value for said every consecutive specified number of characters in said operation request; and

comparing every hash value to stored hash values representing vulnerability patterns.

5. 7. (Currently Amended) A method for protecting an application from executing an illegal or harmful operation request received from a distributed environment, the method comprising the steps of:

designating an application path of an application as restricted,

determining whether an operation request is illegal or harmful to an environment of said application, ~~and~~

preventing said application from executing an illegal or harmful operation request, wherein said step of determining comprises the step of checking said operation request for an existence of an embedded command causing database manipulation~~.~~ and wherein said step of preventing comprises the step of modifying said illegal or harmful operation request into a legal or harmless operation request,

comparing said operation request against stored known vulnerability patterns to determine a match, and

blocking said operation request if said match is found,

wherein said step of comparing comprises the steps of:

converting every consecutive specified number of characters in said operation request into n-bits of binary code;

computing a hash value for said every consecutive specified number of characters in said operation request; and

comparing every hash value to stored hash values representing vulnerability patterns.

6. 17. (Currently Amended) A method for protecting an application from executing an illegal or harmful operation request received from a distributed environment, the method comprising the steps of:

determining whether an operation request is illegal or harmful to an environment of an application;

comparing said operation request against stored known vulnerability patterns to determine a match, and

blocking said operation request if said match is found,

wherein said step of comparing comprises the steps of:

converting every consecutive specified number of characters in said operation request into n-bits of binary code;

computing a hash value for said every consecutive specified number of characters in said operation request; and

comparing every hash value to stored hash values representing vulnerability patterns;

preventing said application from executing an illegal or harmful operation request;

sending a legal or harmless operation request to said application;

generating a reply to said operation request.

7. 23. (Currently Amended) A method for protecting an application from executing an illegal or harmful operation request received from a distributed environment, the method comprising the steps of:

determining whether an operation request is illegal or harmful to an environment of an application,;

comparing said operation request against stored known vulnerability patterns to determine a match, and

blocking said operation request if said match is found,

wherein said step of comparing comprises the steps of:

converting every consecutive specified number of characters in said operation request into n-bits of binary code;

computing a hash value for said every consecutive specified number of characters in said operation request;

comparing every hash value to stored hash values representing vulnerability patterns; and

preventing said application from executing an illegal or harmful operation request, wherein said step of determining comprises the steps of:

identifying a cookie message header in said operation request;

decrypting values in said cookie message header; and

modifying said operation request to reflect said decrypted values.

8. The following is an examiner's statement of reasons for allowance:

The prior art of record discloses that when an illegal or harmful operation is detected it is analyzed and logged. As per claim 5-7, 13, 17 and 23, the prior art of record individually or in combination does not explicitly disclose comparing said operation request against stored known vulnerability patterns to determine a match, and blocking said operation request if said match is found, wherein said step of comparing comprises the steps of: converting every consecutive specified number of characters in said operation request into n-bits of binary code; computing a hash value for said every consecutive specified number of characters in said operation request; and comparing every hash value to stored hash values representing vulnerability patterns; and modify the operation request into legal and harmless operation request in light of other features disclosed in independent claims 5-7, 13, 17 and 23. As per claim 30, 34, 38, and 44, prior art of record individually or in combination fails to disclose applying one or more security pipes to each operation request, wherein the number and types of pipes applied to each operation request are based on said resolved destination node of each operation request in light of other features disclosed in independent claims 30, 34, 38, and 44.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Grimm et al. U.S. Pat. No. 6317868 discloses process for transparently enforcing protection domains and access control as well as auditing operations in software components.

Golan U.S. Pat. No. 5974549 discloses security monitor using sandbox model.

Touboul et al. U.S. Pat. No. 6154844 discloses method for attaching a downloadable security profile to a downloadable.

Touboul et al. U.S. Pat. No. 6092194 discloses method for protecting a computer and a network from hostile downloadable.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100